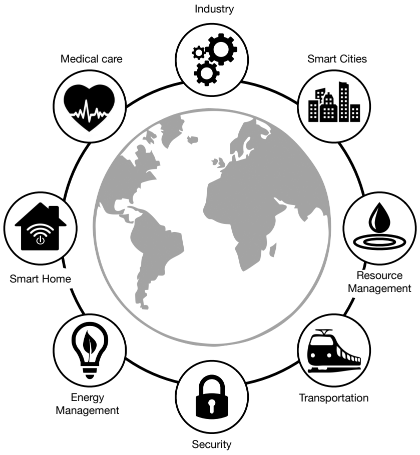
Bachelor Thesis
Secure IoT Device Commissioning

The vision of the Internet of Things (IoT) has become more and more traction, as in the context of Smart Homes and Smart Factories more and more commercial products become available and deployed. However, commissioning of IoT devices is an unsolved problem: The initial setup of secure wireless communication with IoT devices is lacking a trust anchor to build upon. The goal of this thesis is to develop and prototypically implement a secure IoT commissioning protocol.

Current solutions either provide a factory supplied trust anchor or leave the device vulnerable for man in the middle attacks (MITM) during commissioning. While the first approach seems to be secure, it has multiple attack vectors: First, adversaries like the NSA can legally enforce that companies compromise the initial trust anchor while also enforcing to not disclose that trust anchors have been compromised. Secondly, adversaries could break into the infrastructure of a company and compromise the manufacturing process to deploy compromised trust anchors. And lastly, adversaries like the NSA have been known to intercept shipments and compromise the hardware during transit.

Deliberately excepting that a device is vulnerable during commissioning seems to impose only a limited risk, as the time window in which MITM attacks can be mounted is extremely small. However, it has been shown that most the first human reaction to a failing IoT device is to reset and recommission the device [1]. Thus, an adversary can simply jam the communication with the device and wait for the user to recommission the device to successfully mount the MITM attack.



Various Applications of IoT Devices

In this thesis it should be assumed that every IoT device to commission is equipped with a wireless communication interface and status LED. The network interface can communicate both without and – when a credential is available – with transport security.

Project type	Bachelor Thesis	Contact	Marian Buschsieweke
Duration	1 Term	E-Mail	buschsie@ovgu.de
Language(s)	English, German	Room	G29-314
Field	Computer Science	Tel.	+49 391 67-52673

The commissioning should work roughly as follows:

1. The IoT devices gathers entropy, e.g. using the transceiver to gather the RSSI level of background noise in the wireless channel.
2. **The IoT device generates a secure commissioning key, using the gathered entropy**
3. **The IoT device transmits the commissioning key using the status LED**
4. The owner of the IoT device uses the smartphone equipped with a camera to receive the commissioning key
5. **The smartphone uses the commissioning key to encrypt and sign the credential used to securely connect the IoT device**
6. The encrypted and signed credential is send without transport security to the IoT device via its wireless network interface
7. **The IoT devices validates the signature of the received credential and decrypts it**
8. The IoT devices uses the credential to securely connect to the network

Goals

- Develop a specification for steps 2, 3, 5, and 7 in the description above
- Implement a prototype of this specification as a library
- Demonstrate the feasibility of that implementation on an IoT device running RIOT[2]

References

[1] Tobias Zillner. Zigbee Exploited – The good, the bad and the ugly. `https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf`. 2016.

[2] Emmanuel Baccelli and Oliver Hahm and Mesut Güneş and Matthias Wählisch and Thomas Schmidt. RIOT OS: Towards an OS for the Internet of Things. 32nd IEEE International Conference on Computer Communications (INFOCOM). 2013.

Project type	Bachelor Thesis	Contact	Marian Buschsieweke
Duration	1 Term	E-Mail	buschsie@ovgu.de
Language(s)	English, German	Room	G29-314
Field	Computer Science	Tel.	+49 391 67-52673